XML Consortium

～ 第5回 XMLコンソーシアムWeek ～

sPlatプロジェクト
暗号化XMLデータ利用技術についての課題と対策
今後の課題

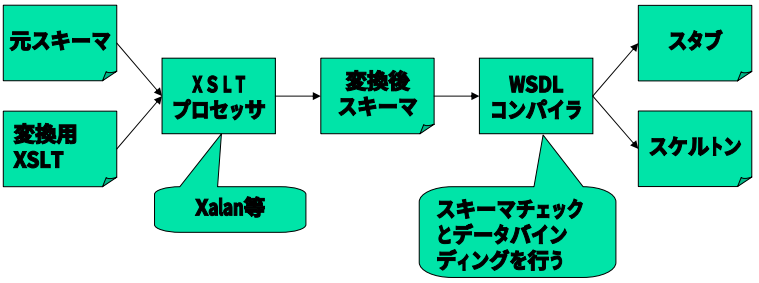
2006年5月24日
XMLコンソーシアム セキュリティ部会
工藤　奈緒美（(株) JIEC）

sPlat今後の課題

- スキーマ変換規則の検証（引き続き）
- ポリシーの設定方法・伝達方法の検討
- 各実装への組み込み方法の検討

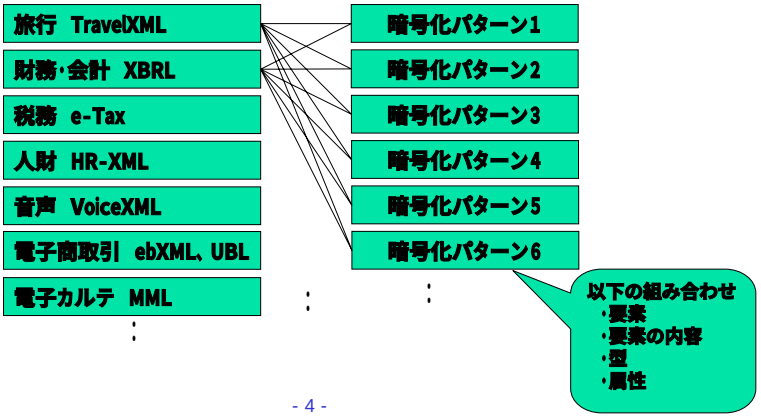
スキーマ変換規則の検証

- 作成したスキーマ変換用XSLTで以下のXMLスキーマを変換し、WSDLコンパイラでスタブ及びスケルトンが正しく作成されることを確認する。



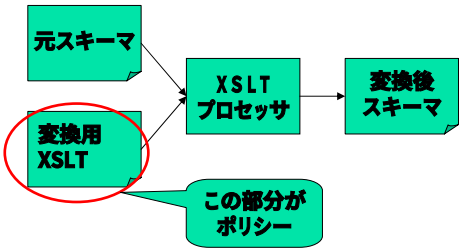
スキーマ変換規則の検証

- 代表的なアプリケーション・スキーマに対し、XML文書を暗号化した場合のスキーマ変換パターンについてテストを行う。



ポリシーの設定と伝達

- あるXML文書のどこを暗号化するのかという決まりをポリシーと呼ぶことにする。
- ポリシーをどのように表現し、保管し、Webサービス業者間でどう伝達するかについて検討する。

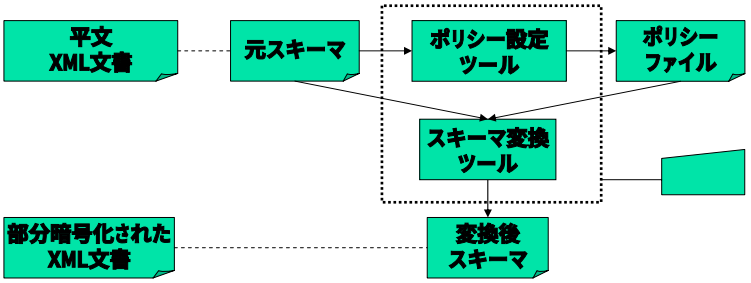


ポリシーの設定

- ポリシーは、個々のWebサービス毎に当事者が決定するビジネス・ルール。
- ポリシーは、スキーマ変換パターンが組み合わされたものとなる。
- XSLTが書けない人でも、XML文書の実際の構造を知らない人でも、ポリシーを設定できるようにしたい。
- 該当XMLスキーマを読み込んで、ポリシーを設定してファイルに保存するような、GUIツールが必要。

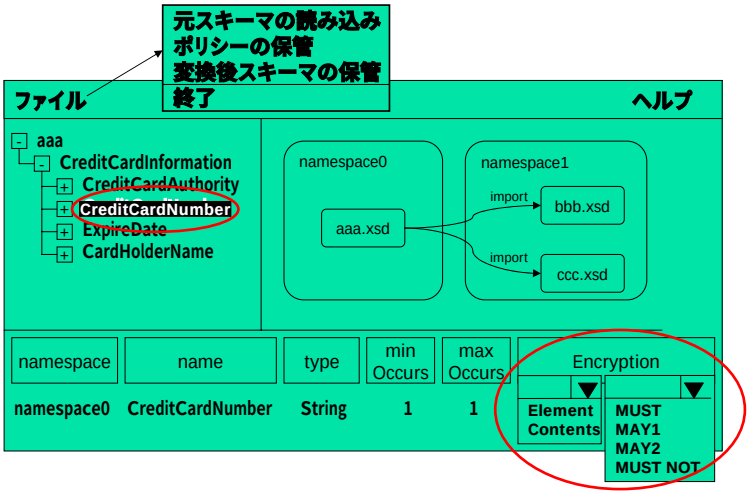
ポリシーの設定

- ポリシー設定用GUIツール
  - 元スキーマを読み込み、設定したポリシーをポリシー・ファイルに書き出す。
  - ポリシー・ファイルを参照して、元スキーマを変換してファイルに書き出す。



ポリシーの設定

- ポリシー設定用GUIツール (例)

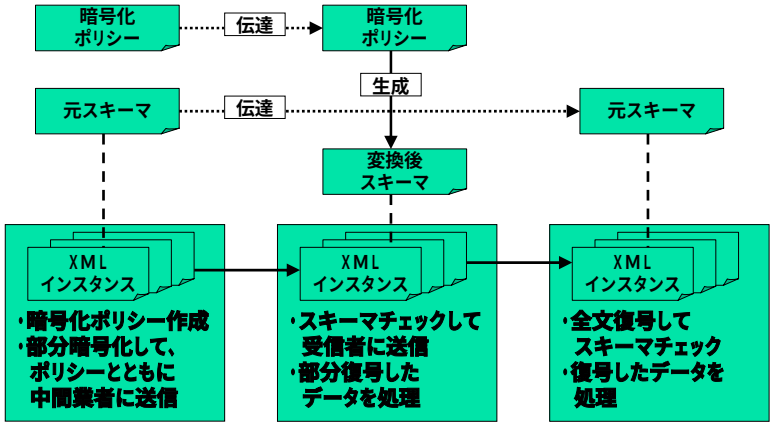


ポリシーの伝達

- スキーマが標準化・公開されていない場合
  - ビジネスルールに従って作成・変更したポリシーを、信頼ある方法で交換する。
  - ポリシーをファイルに保管することにより、ポリシーが変更されてもエンジンを変更する必要はない。
- スキーマが標準化・公開されている場合、ポリシーもセットで公開することにより、伝達を自動化できる。
  - 業種・業界ごとの標準スキーマ
  - 業者ごと、取引ごとのポリシー

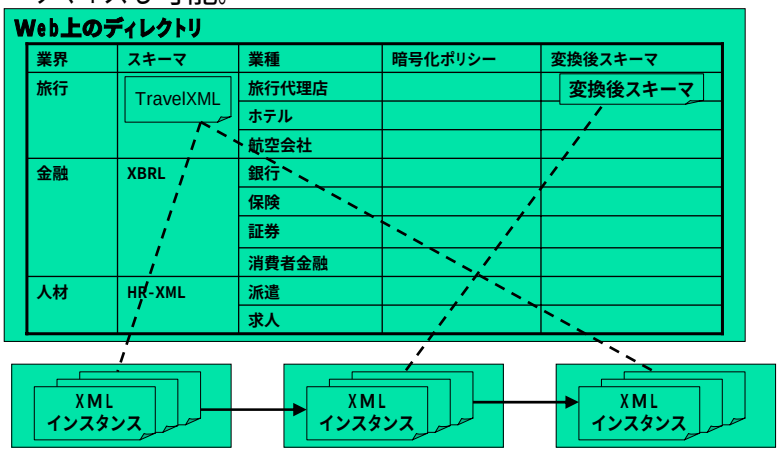
ポリシーの伝達 (非標準化)

- 送信者が暗号化ポリシーを作成する場合の例



ポリシーの伝達（標準化）

- サービス利用者は、該当スキーマと変換後スキーマを適宜ダウンロードして使用する。ポリシーをダウンロードして、カスタマイズも可能。



ポリシー記述形式の標準化

- 異なる組織やアプリケーション間でポリシーを伝達するために、ポリシー記述形式の標準化が必要。
- 標準規格の使用を検討中。
  - WS-SecurityPolicy・・・Webサービスのセキュリティに関する、Webサービス提供者-利用者間の取り決め（ex.どの部分が暗号化されているべきなのか）の記述方法を規定
  - WS-Policy・・・Webサービス提供者-利用者間の取り決めを記述するためのフレームワークを提供
  - WS-PolicyAttachment・・・ポリシーとその主体（ex. WSDLに記述されている個々のメッセージやバインディング）の関連付けの記述方法を規定
- 標準化されたポリシー記述形式を元に、ポリシー設定GUIツールを作成する。

各実装への組み込み

- 作成したツールを、既存の実装と組み合わせて使用する方法を検討